Advanced Malware Protection voor endpoints en het laatst bekeken filter

Inhoud

Inleiding

Dit document beschrijft de verklaring voor de 'last-een' filterbug die wordt verwezen naar CSCvh31177 in Advanced Malware Protection (AMP) voor endpoints.

Bijgedragen door Caly Hess, Cisco Engineer.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Toegang tot de Cisco Advanced Malware Protection voor endpoints

Gebruikte componenten

De informatie in dit document is gebaseerd op de software:

- Cisco Advanced Malware Protection voor endpoints en versie 5.4.2019/917

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Probleem

Het filter "Laatst gezien" van de computerpagina op de console geeft connectors weer die in de afgelopen 24 uur zijn gezien en in de lijst staan.

Oorzaak

De huidige aantrekkingskracht van data van het "Laatste Zeen" is een unieke job elke 24 uur. Hoewel de gegevens die op de pagina Computers en de uitvoer naar CSV voor "Laatste scherm" worden weerspiegeld, real-time zijn, draait het filter zelf de opgeslagen gegevens van die ene taak uit. Dit werd ten uitvoer gelegd om de snelheid van de resultaten te

verhogen, aangezien real-time analyse van de tijdstempels voor grote ondernemingsomgevingen tot time-outs en gegevensblokkering zou kunnen leiden.

Uitleg van "recent bekeken" computers in een filter van meer dan 7 dagen

De machine was 7+ dagen offline, totdat de baan "Laatst gezien" had gewerkt.

Real-World-voorbeeld

- HostA.randomdomain.net had een ongelukkig ongeluk met een koffiebok en het moederbord haalde op 10 augustus geen volledig herstel
- HostA.randomdomain.net zit nu in het reparatiedepot tot 20 september.
- Op 21 septemberst, keert HostA.randomdomain.net terug naar het netwerk 4 uur nadat de "last Seen"-taak was gestart, maar 2 uur voordat de Auditor een Exporteren naar CSV doet van de computers die de afgelopen 30 dagen niet zijn gezien
- HostA.randomdomain.net is nog steeds opgenomen van de "Last Seen"-taak, omdat het meer dan 30 dagen niet is gezien. Ondanks dat deze nu volledig functioneel en koffievrij is, vangt de accountant ze nu op in zijn "inactieve" export

Korte-termijnoplossing

De taak zelf duurt niet 24 uur, maar neemt minimaal 12 uur in beslag. Om de nauwkeurigheid van het filter te verbeteren wordt de automatische herschikking van de taak nadat de vorige is voltooid, uitgevoerd. Naar verwachting zal deze 7-12 uur na het partijvenster doorsnijden.

Langetermijnoplossing

Een totaal herwerk van het "Laatste scherm"-mechanisme dat dichter in de buurt van de realtime ligt wanneer de gegevens worden verzameld. Deze oplossing vereist de invoering van een geheel nieuwe gegevensstructuur die momenteel wordt ontwikkeld met de voorgestelde publicatie in het volgende kalenderjaar.